REMARKS

Applicant respectfully requests reconsideration of the present application in view of the amendments set forth above and the below remarks.

Claims 1, 2, 4-28 and 38-45 are pending in the application.

Applicant believes the claimed invention is clearly patentably distinguishable over the newly cited Juels reference for the reasons set forth below in detail. If after consideration of this Amendment the Examiner does not consider the claimed invention to be patentably distinguishable over the Juels reference (co-authored by a co-inventor of the present application), Applicant respectfully encourages and specifically requests the Examiner to contact the undersigned to arrange a telephone interview to further discuss the office and Juels reference with the undersigned and with inventor Juels.

The Claim Objections

Claims 9, 10, and 16 are objected as being dependent upon a rejection claim. Claim 9 is rewritten in independent form.

The §101 Rejections

The Examiner rejects claims 38 and 39 as being directed to non-statutory subject matter. Applicant amends claim 38 for standard Beauregard claim format and amends claim 39 for consistency with claim 39, as set forth above. Applicant believes the §101 should be withdrawn.

The §112 Rejection

The Examiner rejects claims 1, 17-19, 38, 40, 41, 43 and 45 under 35 U.S.C. §112, second paragraph, alleging that essential steps are omitted. Applicant respectfully requests clarification as to what essential steps are omitted. Any suggestions to amend the claims to address this rejection would be greatly appreciated.

Step (c) of claim 1 requires

"constructing a first sequence of coordinate sets (x_i,y_i), for i in {1,...n}, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element and a second value (y_i) corresponding to a symbol in the codeword, wherein the symbol corresponds to the x_ith symbol in the codeword, wherein an order-invariant fuzzy commitment is formed, the commitment having the property that it may be algorithmically combined with at least one set of values comprising at least one value of the first input element so as to yield the codeword." Applicant believes that performing what is set forth in the claim in fulfilling the specified properties results in an order-invariant commitment.

Applicant respectfully requests that the Examiner contact the undersigned to discuss the §112 rejection should the Examiner maintain the rejection after further consideration.

The Prior Art Rejections

The Examiner rejects claims 1, 2, 4-8, 11, 12, and 14-15 under 35 U.S.C. §102(b) over Juels et al. (Juels), "A Fuzzy Commitment Scheme."

Claim 1 requires:

> a computer-implemented method for creating an order-invariant fuzzy commitment, comprising:
> (a) receiving a first input element comprising a sequence of at least one value $(a_1,..., a_n)$ from a predetermined set;
> (b) generating a codeword of an error-correcting code for generating the commitment;
> (c) constructing a first sequence of coordinate sets (x_i,y_i), for i in {1,...n}, each of the coordinate sets having a first value (x_i) corresponding to a representation of an associated one (a_i) of the at least one value of the first input element and a second value (y_i) corresponding to a symbol in the codeword, wherein the symbol corresponds to the x_ith symbol in the codeword, wherein an order-invariant fuzzy commitment is formed, the commitment having the property that it may be algorithmically combined with at least one set of values comprising at least one value of the first input element so as to yield the codeword; and
> outputting the first sequence.

Applicant submits that Juels clearly does not teach the invention as claimed. Juels does not teach *order invariance*. Nor does Juels teach *a sequence of coordinate sets*.

The Examiner points to Example 2 on pages 32-33 of Juels to teach the constructing step (c) of claim 1. Example 2 teaches a fuzzy commitment scheme in which the witness x' can be 'close' to the original encrypting witness x and achieve decommitment. In Example 2, the "value x' differs from x in two bit *positions*." The difference between x and x' is within the correction threshold of the error correcting code to allow successful decommitment. However, the commitment in Example 2 of Juels is *not order invariant*, as claimed.

As detailed in previous submissions, and discussed with the Examiner in a telephone interview on January 23, 2007, it appears that the Examiner is not giving any patentable weight to the claimed order invariance. As discussed previously, assume for an exemplary embodiment of claim 1 that an original message is (A, B, C, D, E,) and a received message is (E, A, D, C, B), i.e., the ordering is different for each element. Where the commitment is *order invariant* as claimed, element order *does* ***not*** matter. Applicant submits that in no reasonable reading can Juels be considered to teach the claimed "order invariance."

Further, what is produced in Example 2 is not a sequence of coordinate sets, as claimed. Applicant respectfully points out that it appears that the Examiner may be trying to identify the pair (α, δ) as a coordinate pair. However, α is a hash value and does not point to a symbol in the codeword as required by claim 1.

In view of the above, Applicant submits that claim 1 is patentably distinguishable over Juels. For at least the same reasons, Applicant submits that claims 2, 4-28 and 38-45 are also distinguishable.

Accordingly, Applicant respectfully requests a notice of allowance for claims 1, 2, 4-28 and 38-45.

The Examiner is respectfully invited to telephone the undersigning attorney to discuss any matter in furtherance of the present application.

Applicant does not acquiesce to any assertion made by the Examiner not specifically addressed herein.

The Assistant Commissioner is hereby authorized to charge payment of any additional fees associated with this communication or credit any overpayment to Deposit Account No. 500845.

Respectfully submitted,

Dated: March 5, 2008

DALY, CROWLEY, MOFFORD & DURKEE, LLP

By: /Paul D. Durkee/

Paul D. Durkee
Reg. No. 41,003
Attorney for Applicant(s)
354A Turnpike Street - Suite 301A
Canton, MA 02021-2714
Tel.: (781) 401-9988, Ext. 121
Fax: (781) 401-9966
pdd@dc-m.com

63007